KAZEROUNI LAW GROUP, APC
Abbas Kazerounian (SBN: 249203)
ak@kazlg.com
Mona Amini (SBN: 296829)
mona@kazlg.com
245 Fischer Avenue, Suite D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff,
Daroya Isaiah

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

DAROYA ISAIAH, individually an on behalf of all others similarly situated, Plaintiff, vs. LOANDEPOT, INC, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

//

//

//

//

//

//

//

//

//

Plaintiff Daroya Isaiah ("Plaintiff"), by and through their undersigned counsel, files this Class Action Complaint on behalf of themself individually and all others similarly situated, against Defendant loanDepot, Inc. ("loanDepot" or "Defendant"). Plaintiff bases the below allegations on personal information and belief, the investigation of counsel, and states the following:

INTRODUCTION

1. Defendant loanDepot, Inc. is an Irvine, California-based nonbank holding company which sells mortgage and non-mortgage lending products. Founded in 2010, loanDepot has "grown to become the nation's fifth largest retail mortgage lender and the second largest nonbank retail originator, funding more than $275 billion since inception. Today, [loanDepot's] nationwide team of 6,000-plus members assists more than 27,000 customers each month."[1]

2. Pursuant the U.S. Securities and Exchange Commission (SEC) data breach disclosure rules, publicly owned companies operating in the U.S. must comply with a new set of rules requiring them to disclose "material" cyber incidents a Form 8-K report within 96 hours.

3. On January 8, 2024, in a Form 8-K filing[2] with the SEC, loanDepot reported it "recently identified a cybersecurity incident affecting certain of the Company's systems. Upon detecting unauthorized activity, the Company promptly took steps to contain and respond to the incident, including launching an investigation with assistance from leading cybersecurity experts, and began the process of notifying applicable regulators and law enforcement." The report further announced, "Though our investigation is ongoing, at this time, the Company has determined that the unauthorized third party activity included access to certain Company systems and the encryption of data. In response, the Company shut down certain systems and continues to implement measures to secure its business

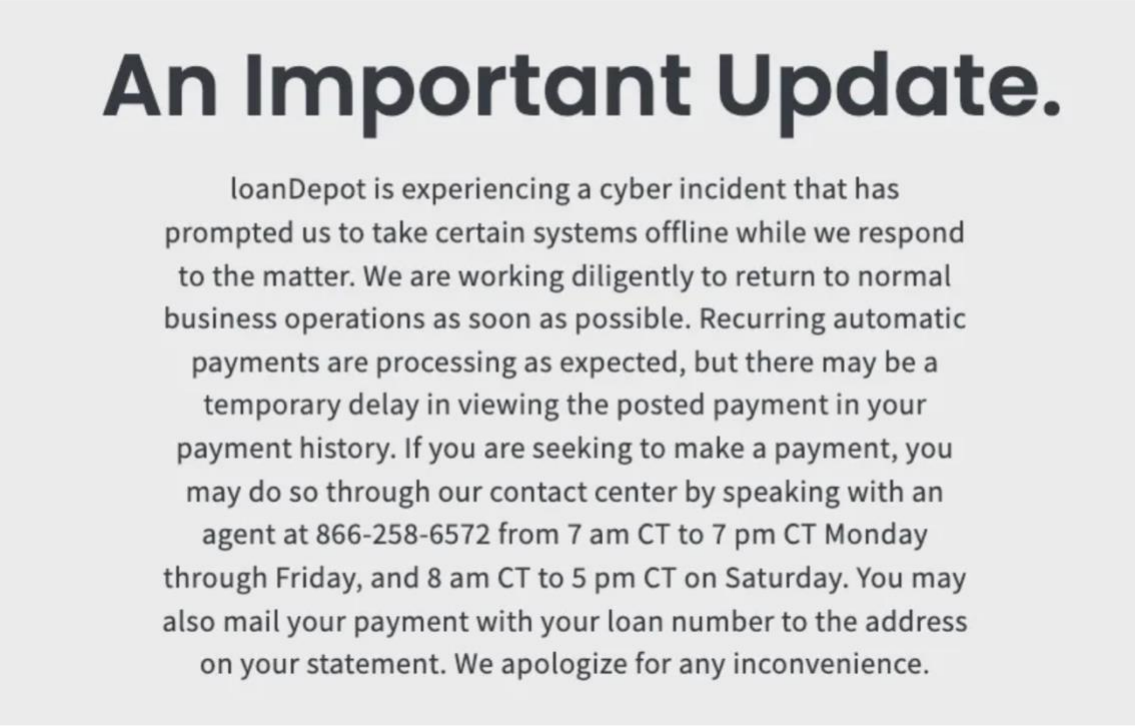
[1] https://www.loandepot.com/about
[2] *See* https://investors.loandepot.com/financials/sec-filings/default.aspx

operations, bring systems back online and respond to the incident."[3]

4. Defendant has not yet disclosed the total number of customers impacted by the "cybersecurity incident," and it is unclear what sensitive personal information and/or PII was disclosed, accessed, and/or acquired from Defendant's systems by unauthorized third parties.

5. Upon information and belief, Plaintiff's and the Class members' unencrypted sensitive personal information, or PII, which was collected, maintained, and stored by loanDepot, was acquired, or reasonably believed to have been acquired, by an unauthorized person in the "cybersecurity incident" disclosed by Defendant (the "Data Breach").

6. Following the Data Breach, loanDepot's website, including its customer portals, appeared to be non-functional, and the following error message appeared on loanDepot's customer login page, asking customers seeking to make a payment to call or mail in their payment instead.[4]



[3] *See* loanDepot Form 8-K Filing: https://d18rn0p25nwr6d.cloudfront.net/CIK-0001831631/446c437f-153f-425d-adc6-bf37155d6e91.pdf
[4] https://techcrunch.com/2024/01/08/loandepot-outage-suspected-ransomware-attack/

7. Because Defendant holds sensitive personal information about its customers, and PII including social security numbers, and financial and bank account information, Plaintiff and the Class (defined below) have been placed in an imminent and continuing risk of harm from fraud, identity theft, and related harm caused by the Data Breach and should remain vigilant for any signs of fraud or identity theft for the indefinite future.

8. As a result of Defendant's conduct, Plaintiff and the Class have and will be required to continue to undertake time-consuming and often costly efforts to mitigate the actual and potential harm caused by the Data Breach. This includes efforts to mitigate the breach's exposure of their PII, including by, among other things, placing freezes and setting alerts with credit reporting agencies, contacting financial institutions, closing, or modifying financial accounts, reviewing, and monitoring credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate records.

9. Defendant has had prior notice of its inadequate data security procedures and practices. In fact, less than a year ago, in May 2023, loanDepot disclosed a data breach resulting from a cyberattack in August 2022 that exposed loanDepot customer data.

10. Plaintiff therefore brings this Class Action seeking injunctive relief and damages against Defendant, individually and on behalf of all other persons whose personal information was impacted by the Data Breach resulting from loanDepot's inadequate data security procedures and practices.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005. Subject matter jurisdiction is proper because: (1) the amount in controversy in this class action exceeds five million dollars ($5,000,000), excluding interest and costs; (2) there are

more than 100 Class members; (3) at least one member of the Class is diverse from the Defendant; and (4) the Defendant is not a government entity.

12. This Court has personal jurisdiction over Defendant because Defendant's acts or omissions and false or misleading representations regarding the security of Plaintiff's and Class members' PII have impacted Plaintiff, who resides in this District; and Defendant is a corporation that maintains a headquarters or principal place of business in Irvine, California, and transacts business from in this District.

13. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part events and injury giving rise to Plaintiff's claims occurred in or originated from this District and Defendant does business and transact business in this District.

PARTIES

14. Plaintiff is and has been at all relevant times a citizen and resident of Adelanto, California.

15. Defendant is a corporation organized under the laws of Delaware with a corporate headquarters, or principal place of business, located in Irvine, California.

FACTUAL BACKGROUND

A. Defendant Collected, Maintained, and Stored PII.

16. In providing mortgage and non-mortgage lending products and related financial services, Defendant collect sensitive personal information from customers. This information includes name, email address, username, password, social security number, phone number, mailing address, financial information, tax information, credit history, employment information, drivers' license information, insurance information, marital status, and other personal and highly sensitive information a person might provide when trying to procure a mortgage or loan. Defendant hosts a large repository of sensitive personal information maintained for its customers and received from its customers, including Plaintiff and the Class.

B. Defendant Knew it Needed to Protect Customers' Sensitive Personal Information and Committed to Protecting their PII.

17. Defendant has a Privacy Policy on its website which clearly states, "loanDepot® values your patronage and protecting your confidential information is a priority. Our policies and procedures reinforce the fact that loanDepot strongly believes in protecting the confidentiality and security of the information we collect about you as a customer, potential customer, or former customer."[5]

18. Defendant's Privacy Policy further represents that loanDepot has "adopted the following policies and procedures to safeguard the personal information about you in our possession."[6]

19. As a condition of receiving a mortgage, loan, or other financial services, loanDepot collects and requires that its customers provide loanDepot with highly sensitive personal information. In its "Privacy Policy", loanDepot includes the following representations:[7]

> **Our Privacy Pledge**
>
> - We do not sell or rent customer information.
> - We share customer information with certain employees and with companies providing services on our behalf in order to service your needs.
> - Our policy is to require all employees and companies providing services on our behalf to keep customer information confidential.
> - Our privacy policy applies to potential customers as well as current and former customers.
>
> **Safeguarding Personally Identifiable Information**
>
> - We have adopted policies and procedures designed to protect your personally identifiable information from unauthorized use or disclosure.
> - We have implemented physical, electronic and procedural safeguards to maintain confidentiality and integrity of the personal information in our possession and to guard against unauthorized access. These include among other things, procedures for controlling access to customer files, building security programs and information technology security measures such as the use of passwords, firewalls, virus prevention and use detection software.

[5] https://investors.loandepot.com/privacy-policy/default.aspx
[6] *Id.*
[7] *Id.*

- We continue to assess new technology as it becomes available and to upgrade our physical and electronic security systems as appropriate.
- Our policy is to permit employees to access your personal information only if they have a business purpose for using such information, such as administering, providing or developing our products or services.
- Our policy, which governs the conduct of all of our employees, requires all employees to safeguard personally identifiable information about the consumers and customers we serve or have served in the past.

loanDepot Security Policy

loanDepot takes strong steps to safeguard your personal and sensitive information through industry standard physical, electronic and operational policies and practices. All data that is considered highly confidential data can only be read or written through defined service access points, the use of which is password-protected. The physical security of the data is achieved through a combination of network firewalls and severs with tested operating systems, all housed in a secure facility. Access to the system, both physical and electronic, is controlled and sanctioned by a high-ranking manager.

Information We Collect About You

We collect information about you to help us serve your financial needs, to provide you with quality products and services and to fulfill legal and regulatory requirements. We consider non-public information about you in our possession to be personally identifiable information, even if you cease to be a customer. The personally identifiable information we collect about you may include among other things:

- Identifying information, such as your name, age, address, phone number and social security number
- Employment information
- Financial information such as your income, assets and liabilities, as well as information about your savings, investments, insurance and business.

20. Based on such policies and representations, Defendant knew it needed to protect the privacy and safeguard the sensitive personal information and PII of its potential, former, and customers, including Plaintiff and the Class members.

C. Defendant's Inadequate Data Security Measures Exposed Customers' Sensitive Personal Information. And PII.

21. In or around January 4, 2024, a malicious actor gained unauthorized access to Defendant's company data systems. By doing so, the unauthorized third party gained access to the sensitive personal, financial, and other confidential information of loanDepot's potential, former, and customers, including Plaintiff and the Class members.

22. Upon information and belief, the actors accessed and acquired substantial amounts of Plaintiff's and the Class's sensitive personal information, including their PII. This data included highly sensitive personal information such as names, addresses, social security number, employment information, and financial information.

23. Given that Defendant purposefully obtained and stored the PII of Plaintiff and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendant was obligated to implement reasonable measures to prevent and detect cyberattacks. This includes measures recommended by the Federal Trade Commission ("FTC") and promoted by data security experts and other agencies. This obligation stems from the foreseeable risk of a data breach given that Defendant collected, stored, and had access to a swath of highly sensitive consumer records and data and, additionally, because other highly publicized data breaches at different institutions put Defendant on notice that the highly personal data they stored, or allowed other entities to store via a services contract or relationship, might be targeted by cybercriminals.

24. Despite the highly sensitive nature of the personal information Defendant obtained, created, and stored, and the prevalence of data breaches at financial institutions like Defendant or related businesses, Defendant inexplicably failed to implement and maintain reasonable and adequate security procedures and practices to safeguard the PII of Plaintiff and the Class. The Data Breach itself and information Defendant have disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, and the sensitive nature of the impacted data, collectively demonstrate Defendant failed to implement reasonable measures to prevent the Data Breach and the exposure of highly sensitive customer information.

//

//

D. Exposure of PII and other Sensitive Personal Information Created a Substantial Risk of Harm.

25. The personal and financial information of Plaintiff and the Class is valuable and has become a highly desirable commodity to data thieves.

26. Upon information and belief, Plaintiff's and the Class members' sensitive personal information and/or PII has been made available on the dark web as a result of the Data Breach.

27. Defendant's failure to reasonably safeguard Plaintiff's and the Class's sensitive PII has created a serious risk to Plaintiff and the Class, including both a short-term and long-term risk of identity theft and other fraud.

28. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

29. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[8]

30. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

31. Purchasers of PII use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional PII from the victim, as well as PII from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass

[8] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com

financial data and tangible money, along with unreported emotional harms.

32. The FBI's Internet Crime Complaint (IC3) 2019 report estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help stop fraudulent transactions and mitigate losses.

33. The FTC has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour reiterated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[9]

34. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;
(2) retaining payment card information only as long as necessary;
(3) properly disposing of personal information that is no longer needed or can be disposed of pursuant to relevant state and federal laws;
(4) limiting administrative access to business systems;
(5) using industry tested and accepted methods;
(6) monitoring activity on networks to uncover unapproved activity;
(7) verifying that privacy and security features function properly;
(8) testing for common vulnerabilities; and
(9) updating and patching third-party software.[10]

[9] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable.

[10] *Start With Security, A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

35. The United States Cybersecurity & Infrastructure Security Agency ("CISA"), and other federal agencies, recommend similar and supplemental measures to prevent and detect cyberattacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

36. The FTC cautions businesses that failure to protect PII and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money, and patience to resolve the fallout.[11] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like Defendant failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

E. Plaintiff's and the Class's PII are Valuable.

37. Birth dates, Social Security Numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[12]

38. For that reason, cybercriminals on the dark web are able to sell data like Social Security Numbers for large profits.

39. Consumers place a considerable value on their PII and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their PII, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective

---

[11] Taking Charge, What to Do if Your Identity is Stolen, FTC, https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0014-identity-theft.pdf.

[12] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

"protection against error, improper access, and secondary use of personal information is worth" between $30.49 and $44.62.[13] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

40. Upon information and belief, Defendant's Data Breach exposed a variety of Plaintiff's and the Class members' data, including their social security numbers, financial information, and other sensitive personal information or PII.

41. The Social Security Administration ("SSA") warns that a stolen Social Security Number can lead to identity theft and fraud: "Identity thieves can use your number and your credit to apply for more credit in your name."[14] If the identity thief applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

42. Social Security Numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

43. Plaintiff entrusted her personal information and PII to loanDepot in connection with its mortgage, loan, and financial services. Plaintiff's personal information, including Plaintiff's PII, was entrusted to loanDepot with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Plaintiff would not have provided her PII to Defendant had she known that loanDepot would not undertake reasonable data security measures.

44. Since learning of the Data Breach, Plaintiff has undertaken reasonable efforts to mitigate the impact of the Data Breach, including but not limited to

---

[13] 11-Horn Hann, Kai-Lung Hui, et al, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf

[14] Social Security Administration, Identity Theft and Your Social Security Number, https://www.ssa.gov/pubs/EN-05-10064.pdf

reviewing her loanDepot account, financial account statements, and/or credit reports for any indications of actual or attempted identity theft or fraud. As a result of the Data Breach, Plaintiff will continue to spend valuable time for the remainder of her life, to mitigate the impact of the Data Breach, and dispute and rectify the fraud and/or damage to her credit reputation experienced as a result of the Data Breach which Plaintiff otherwise would have spent on other activities, including but not limited to leisure, work, and/or recreation.

45. Since the Data Breach, Plaintiff has also experienced a significant increase in SPAM phone calls or text messages; and noticed strange information or accounts on her credit report, which Plaintiff believes could be attributed to the Data Breach.

46. Plaintiff and the Class have suffered invasion of privacy, and now face years of monitoring their financial and personal records with a high degree of scrutiny to mitigate present, imminent and impending injury arising from the increased risk of identity theft and fraud caused by the Data Breach. Plaintiff and the Class has incurred and will continue to incur this damage in addition to any fraudulent use of their sensitive personal information for years to come.

CLASS ALLEGATIONS

47. Plaintiff brings this action on behalf of themself individually and on behalf of all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> ***All individuals whose data was impacted or otherwise compromised by the Data Breach disclosed or reported by loanDepot in January 2024.***

48. In addition, Plaintiff also seeks to represent a California Subclass defined as follows:

> ***All California residents whose PII was impacted or otherwise compromised by the Data Breach initially disclosed or reported by loanDepot in January 2024.***

49. The Nationwide Class and the California Subclass are together referred to herein as the "Class."

50. Excluded from the Class are Defendant and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

51. Plaintiff reserves the right to, after conducting discovery, modify, expand, or amend the above Class definition or to seek certification of a class or Classes defined differently than above before any court determines whether certification is appropriate.

52. **Numerosity.** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are thousands of members of the Class, if not more. The number of impacted individuals remains unknown and unreported, and Plaintiff believe additional entities and persons may have been affected by the Data Breach. The precise number of Class members, however, is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

53. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Defendant knew or should have known that their data environment and cybersecurity measures, or those created by corporate service providers, created a risk of a data breach;

b. Whether Defendant controlled and took responsibility for protecting Plaintiff's and the Class's data when they solicited that data, collected it, stored and maintained such data it on its servers, and/or authorized employees, vendors, or any third parties to access, collect, or store that data;

c. Whether Defendant's security measures were reasonable considering the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;

d. Whether Defendant owed Plaintiff and the Class a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected, stored, and maintained from Plaintiff and Class members;

e. Whether Defendant's failure to adequately secure Plaintiff's and the Class's data constitutes a breach of its duty to institute reasonable security measures;

f. Whether Defendant's failure to implement reasonable data security measures allowed the breach of their data systems to occur and caused the theft of Plaintiff's and the Class's data;

g. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of Defendant's failure to reasonably protect its data systems; and

i. Whether Plaintiff and the Class are entitled to damages and/or equitable relief and/or declaratory relief.

54. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff and the Class members are persons who provided data to Defendant, whose data was collected, stored, and maintained by

Defendant and resided on Defendant's servers or systems, and whose personally identifying information was exposed in Defendant's Data Breach. Plaintiff's injuries are similar to other Class members and Plaintiff seeks relief consistent with the relief due to the Class.

55. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and committed to pursuing this matter against Defendant to obtain relief for themselves and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

56. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

57. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CAUSES OF ACTION

COUNT I

Negligence

58. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

59. Defendant owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiff and the Class. This duty arises from multiple sources.

60. Defendant owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target Defendant's data systems and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed.

61. Defendant further knew or should have known that if hackers breached their data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, Defendant knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Defendant's unsecured, unreasonable data security measures.

62. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendant to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Defendant's duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant failing to use reasonable measures to protect sensitive data. Defendant, therefore, were required and obligated to take reasonable measures to

protect data they possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendant's duty to adequately protect sensitive personal information. By failing to implement reasonable data security measures, Defendant acted in violation of § 5 of the FTCA.

63. Also, the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100, imposes an affirmative duty on businesses, such as Defendant, which maintain personal information about California residents, to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach impacting Plaintiff's and the Class members' sensitive personal information, including PII.

64. Defendant is obligated to perform their business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendant to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

65. Finally, Defendant assumed the duty to protect sensitive data by soliciting, collecting, and storing consumer data and, additionally, by representing to consumers, including its potential, former, and current customers, that it lawfully complied with data security requirements and had adequate data security measures in place to protect the confidentiality of Plaintiff's and the Class's private and sensitive personal information.

66. Defendant breached their duty to Plaintiff and the Class by implementing inadequate and/or unreasonable data security measures that they knew or should have known could cause a Data Breach. Defendant knew or should have known that hackers might target sensitive data Defendant solicited and collected, which was later collected and stored by Defendant, on customers and, therefore, needed to use reasonable data security measures to protect against a Data Breach.

Indeed, Defendant acknowledged they were subject to certain standards to protect data and utilize other industry standard data security measures.

67. Defendant were fully capable of preventing the Data Breach. Defendant knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. Defendant particularly were on notice of inadequate data security measures as loanDepot had experienced a data breach, which it announced nearly a year ago in May 2023. Defendant thus failed to take reasonable measures to secure its systems, leaving Plaintiff and the Class members' sensitive personal information and/or PII vulnerable to a breach.

68. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

69. Plaintiff and the Class members have suffered damages as a result of Defendant's negligence, including actual and concrete injuries and will suffer additional injuries in the future, including economic and non-economic damages from invasion of privacy, costs related to mitigating the imminent risks of identity theft, time and effort related to mitigating present and future harms, actual identity theft, the loss of the benefit of bargained-for security practices that were not provided as represented, and the diminution of value in their PII.

COUNT II

Negligence Per Se

70. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

71. Defendant's unreasonable data security measures constitute unfair or deceptive acts or practices in or affecting commerce in violation Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, it requires

businesses to institute reasonable data security measures and breach notification procedures, which Defendant failed to do.

72. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to use reasonable measures to protect users' sensitive data.

73. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the sensitive nature and amount of data Defendant stored on their users and the foreseeable consequences of a Data Breach should Defendant fail to secure their systems.

74. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

75. In addition, the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.100, *et seq*. requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." 1798.81.5(c).

76. Defendant failed to comply with the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and Class members' PII. Defendant failed to implement reasonable security procedures and practices to prevent an attack on its servers or systems by hackers and to prevent unauthorized access and exfiltration of Plaintiff's and Class members' PII as a result of the Data Breach.

77. Plaintiff and the Class are within the class of persons Section 5 of the FTC Act, the CCPA, and other similar state statutes, was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act. The CCPA, and other similar state statutes, was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

78. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III

Breach of Contract

79. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

80. Plaintiff and Class members entered into a valid and enforceable contract through which they were required to turn over their sensitive personal information to Defendant in exchange for services.

81. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class members' sensitive personal information to any third parties without their consent.

82. Defendant's Privacy Policy published on loanDepot's website[15] memorialized the rights and obligations of Defendant and its customers. This document and/or the representations contained therein was provided to Plaintiff and Class members in a manner in which it became part of the agreement for services with Defendant.

83. Aside from state and federal laws, regulations, and industry standards, through the Privacy Policy, Defendant committed to protecting the privacy and

[15] https://investors.loandepot.com/privacy-policy/default.aspx

security of the sensitive personal information and promised to never share Plaintiff's and Class members' PII except under certain limited circumstances.

84. Plaintiff and Class members fully performed their obligations under their contracts with Defendant. However, Defendant failed to secure, safeguard, and/or keep private Plaintiff's and Class members' PII, and therefore Defendant breached its contracts with Plaintiff and Class members.

85. Despite Defendant's knowledge of its inadequate data security measures that resulted in at least one previously known August 2022 data breach announced to customers in May 2023, Defendant continued to store and maintain possession and control of Plaintiff's and Class members' PII, which predictably led to criminal third parties accessing, copying, and/or exfiltrating Plaintiff's and Class members' PII without permission through Defendant's failure to reasonably safeguard such data in order to prevent the Data Breach.

86. Defendant's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTC Act, resulted in Defendant providing services to Plaintiff and Class members that were of a diminished value and in breach of its contractual obligations to Plaintiff and Class members.

87. As a result, Plaintiff and Class members have been harmed, damaged, and/or injured as described herein, including by Defendant's failure to fully perform its part of the agreement with Plaintiff and Class members.

88. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members suffered and will continue to suffer damages in an amount to be proven at trial.

89. In addition to monetary relief, Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen their data security monitoring and supervision procedures, conduct periodic audits of those procedures, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT IV

Breach of Implied Contract

90. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

91. Defendant provides mortgages, loans, or other financial services to Plaintiff and Class members. Plaintiff and Class members formed an implied contract with Defendant regarding the provision of those services through its collective conduct, including by Plaintiff and Class members providing their PII to Defendant in exchange for the services offered.

92. Through Defendant's offering of these lending services, it knew or should have known that it needed to protect Plaintiff's and Class members' confidential PII in accordance with their own policies, practices, and applicable state and federal law.

93. As consideration, Plaintiff and Class members turned over valuable PII relying on Defendant to securely maintain and store their PII in return and in connection with their services.

94. Defendant accepted possession of Plaintiff's and Class members' PII for the purpose of providing its services, including data security, to Plaintiff and Class members.

95. In delivering their PII to Defendant in exchange for their services, Plaintiff and Class members intended and understood that Defendant would adequately safeguard their PII as part of those services.

96. Defendant's implied promises to Plaintiff and Class members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to PII, including its business associates, vendors, and/or suppliers, also protect the confidentiality of that data; (2) taking steps to ensure that the PII that is placed in the control of its business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained

employees, business associates, vendors, and/or suppliers; (4) designing and implementing appropriate retention policies to protect the PII against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

97. Plaintiff and Class members would not have entrusted their PII to Defendant in the absence of such an implied contract.

98. Had Defendant disclosed to Plaintiff and the Class that they did not have adequate data security and data supervisory practices to ensure the security of their sensitive data, including but not limited to Defendant's decision to continue to collect, store, and maintain Plaintiff's and Class members' PII despite knowledge of loanDepot's previous data breach, Plaintiff and Class members would not have agreed to provide their PII to Defendant.

99. As providers of mortgage, lending, and financial services, Defendant recognized (or should have recognized) that Plaintiff's and Class member's PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the Class.

100. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures and supervision of its systems and networks, as well as its vendors, business associates, and/or suppliers, to secure Plaintiff's and Class members' PII.

101. A meeting of the minds occurred, as Plaintiff and Class members agreed, *inter alia*, to provide their accurate and complete sensitive personal information to Defendant in exchange for Defendant agreement to, *inter alia*, protect their PII.

102. Plaintiff and Class members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT VI

Breach of Fiduciary Duty

103. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

104. A relationship existed between Plaintiff and Class members and Defendant in which Plaintiff and Class members put their trust in Defendant to protect the PII of Plaintiff and Class members and Defendant accepted that trust.

105. Defendant breached the fiduciary duties that they owed to Plaintiff and Class members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the PII of Plaintiff and Class members.

106. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and Class members.

107. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and Class members would not have occurred.

108. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class members.

109. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff are entitled to and demand actual, consequential, and nominal damages, and injunctive relief.

COUNT VII

Unjust Enrichment

110. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

111. Plaintiff and Class members conferred a benefit on Defendant. Specifically, they provided Defendant with their PII, which PII has inherent value. In exchange, Plaintiff and Class members should have been entitled to Defendant's adequate protection and supervision of their PII, especially in light of their special

relationship.

112. Defendant knew that Plaintiff and Class members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class members' PII for business purposes.

113. Defendant failed to secure Plaintiff's and Class members' PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their PII provided.

114. Defendant acquired the PII through false promises of data security and/or inequitable record retention as it failed to disclose the inadequate data security practices, procedures, and protocols previously alleged.

115. If Plaintiff and Class members had known that Defendant would not use adequate data security practices, procedures, and protocols to secure their PII, they would have endeavored to make alternative mortgage servicing choices that excluded Defendant.

116. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred upon them.

117. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and/or will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which

remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

118. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from their wrongful conduct alleged herein. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

119. Plaintiff and Class members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VIII

Declaratory and Injunctive Relief

120. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

121. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

122. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue

to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

123. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continue to owe a legal duty to secure the sensitive personal information with which they are entrusted, specifically including information obtained from its customers, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. Defendant breached, and continue to breach, their legal duty by failing to employ reasonable measures to secure their customers' personal information; and,

c. Defendant's breach of their legal duty continues to cause harm to Plaintiff and the Class.

124. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its users' data.

125. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

126. The hardship to Plaintiff and the Class if an injunction does not issue

exceeds the hardship to Defendant if an injunction is issued.

127. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

128. Wherefore, Plaintiff, on behalf of themself individually and the Class, requests that this Court award relief as follows:

a. An order certifying the Class and designating Plaintiff as the Class Representative and Plaintiff's counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages and equitable relief with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs as allowed by law; and

f. Any other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

Plaintiff hereby demand a jury trial for all claims and issues so triable.

Dated: January 19, 2024

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: *s/ Abbas Kazerounian*

Abbas Kazerounian
Mona Amini
245 Fischer Avenue, Suite D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
Email: ak@kazlg.com
Email: mona@kazlg.com

Attorneys for Plaintiff